Journal of Crime and Justice

ISSN: 0735-648X (Print) 2158-9119 (Online) Journal homepage: https://www.tandfonline.com/loi/rjcj20

Stolen account credentials: an empirical comparison of online dissemination on different platforms

Renushka Madarie, Stijn Ruiter, Wouter Steenbeek & Edward Kleemans

To cite this article: Renushka Madarie, Stijn Ruiter, Wouter Steenbeek & Edward Kleemans (2019) Stolen account credentials: an empirical comparison of online dissemination on different platforms, Journal of Crime and Justice, 42:5, 551-568, DOI: 10.1080/0735648X.2019.1692418

To link to this article: https://doi.org/10.1080/0735648X.2019.1692418

Published online: 10 Dec 2019.

JOURNAL OF CRIME AND JUSTICE
2019, VOL. 42, NO. 5, 551–568
https://doi.org/10.1080/0735648X.2019.1692418

OPEN ACCESS

Stolen account credentials: an empirical comparison of online dissemination on different platforms

Renushka Madarie[a,b], Stijn Ruiter[a,b], Wouter Steenbeek[a] and Edward Kleemans[c]

[a]Netherlands Institute for the Study of Crime and Law Enforcement, Amsterdam, The Netherlands; [b]Department of Sociology, Utrecht University, Utrecht, The Netherlands; [c]Faculty of Law, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

ABSTRACT

Account hijacking, i.e. illegitimately accessing someone else's personal online account, is on the rise and affects not only financial accounts, but the full spectrum of online accounts. To gain more insight in the illicit act of online dissemination of stolen account credentials, we systematically examined how such credentials were offered on three different types of online platforms where stolen credentials were disseminated and how offers varied by platform. We used web scrapes of these platforms for our comparative analyses. Our results demonstrate variation by platform in the type of information on accounts and account holders offered, the average asking price for credentials, and rules and services following a transaction. We conclude with policy implications and suggestions for future research based on the criminal event perspective.

KEYWORDS
Stolen account credentials; criminal event perspective; illicit online markets; web scrapes

Introduction

With the expansion of and increased reliance on digital systems and networks, more and more data are stored in virtual places, such as companies' cloud services. Although this has substantial practical benefits, such as easier sharing and quicker retrieval of information, increased reliance on online storage and networks also leads to more points of access that could be corrupted. Furthermore, end-users do not always apply sufficient measures to protect the data they store online. For instance, people often use rather weak passwords or the same password for multiple accounts (Das et al. 2014; Golgowski 2017). This lack of proper security measures also increases opportunities for data theft. In fact, websites like *haveibeenpwned.com* demonstrate that vast numbers of stolen account credentials have been disseminated online the past few years. Account credentials are data providing direct access to a personal online account, such as an e-mail account or a webshop account. Usually, account credentials are a combination of a username and a password.

Most criminological research into stolen data so far has focused on stolen financial data, such as credit card information (e.g., Holt, Smirnova, and Chua 2016a and 2016b). However, account credentials apply to a wide range of different types of accounts instead of only financial accounts. Moreover, account credentials might be more profitable for data thieves, as evidenced by being sold at higher prices on illicit markets online than stolen financial data (Shulman 2010).

Stolen account credentials can be used for account hijacking, i.e. illegitimately accessing someone else's personal online account. Hijacked accounts can subsequently be exploited in various ways. They can be used as stepping stones for hijacking other accounts of the same user when the same credentials were used for multiple accounts (Bursztein et al. 2014). Account hijackers can also extend

CONTACT Renushka Madarie rmadarie@nscr.nl

their crimes to the account holder's contacts through identity theft and sending spam e-mails (Shay et al. 2014). Account holders of hacked dating sites have also been blackmailed (Onaolapo, Mariconti, and Stringhini 2016) and some hijackers break into webshop accounts to buy expensive goods and resell these goods for cash (Detrixhe 2018).

Even though accounts can be exploited in different ways, data thieves do not always exploit login credentials themselves. Instead, they sometimes decide to disseminate the credentials on online platforms (Herley and Florêncio 2010; Hutchings and Holt 2015; Motoyama et al. 2011). The dissemination of stolen credentials and the wider demand for stolen data has resulted in thriving online markets as well as platforms where stolen data are distributed for free (High-Tech Bridge 2014). Previous research on underground markets largely focused on the economy of these markets (e.g., Allodi 2017; Benjamin et al. 2015; Franklin et al. 2007; Holt, Smirnova, and Chua 2016a; Kigerl 2018) or on how trust issues in these anonymous environments are solved through reputation systems and admission procedures (e.g., Dupont et al. 2017; Mell 2012; Motoyama et al. 2011).

Although the literature on underground markets provides valuable insights into the social and economic forces hypothesised to affect behaviours of market participants, this body of literature is hardly embedded in criminological theory. Furthermore, even though products on hacking forums have been analysed several times, few studies to date specifically focused on the market for account credentials.

In this study, we aim to gain a better understanding of the illicit dissemination of stolen account credentials. We expand on previous research by comparing different types of online platforms where stolen credentials are disseminated, how such credentials are disseminated through posts, and how this varies by type of platform. This study is mainly descriptive and guided by the criminal event perspective (CEP; Meier, Kennedy, and Sacco 2001). This perspective serves as a tool enabling researchers to study different aspects of criminal events in conjunction. Rather than focusing only on, for instance, offenders or victims, as is common in most criminological research, the CEP directs attention to the bigger picture of the event, including its precursors and aftermath.

In the next section, we elaborate on the CEP and provide a literature review of different types of online platforms and the dissemination of stolen data on such platforms. Subsequently, the research methods are detailed and the empirical findings are reported. In the conclusion and discussion section, we reflect on the findings and suggest policy implications and directions for future research.

Theoretical framework

When attempting to explain crime, criminologists traditionally focus on either offenders, victims, or situational factors (Meier, Kennedy, and Sacco 2001). Meier, Kennedy, and Sacco (2001) argue that different crime related factors should be studied in conjunction more often. By doing so, more complete explanations and new theories could be developed that are more attentive to the ways different crime elements are connected. Furthermore, different theoretical questions may surface that would be less obvious when studying crime factors separately. To this end, they developed the criminal event perspective (CEP), a heuristic designed to direct focus from just one part to the bigger picture of the criminal event.

To obtain a more complete picture of the relationship between different elements of criminal events, researchers have to gather data on a multitude of elements. Previous studies deployed CEP in various ways for a range of crimes. For instance, Pino (2005) used CEP to conduct a qualitative case study on serial rape. Weaver et al. (2004) examined how factors identified through the use of CEP (e.g., location, time, and victim characteristics) related to the lethality of violent encounters. Grommon and Rydberg (2014) used CEP in their interdisciplinary study of criminological and public health correlates of firearm injury severity. Finally, Anderson and Meier (2004) rightfully note that there is also a plethora of studies examining interactions between different crime elements without explicitly mentioning CEP.

The aim of the present descriptive study is to gain more insight into the illicit act of disseminating stolen account credentials online. Two types of actors are involved: suppliers offering credentials and potential hijackers looking to exploit accounts. Although there are no direct victims in this act, stolen credentials can be used to victimise people and organisations. The settings (i.e., platforms) where stolen credentials are disseminated sometimes enable interaction between suppliers and potential buyers. On those platforms, suppliers present their products and interested potential hijackers can subsequently show their interest by, for instance, ordering an item for sale or asking for more information. The interplay between suppliers and hijackers on these platforms results in a typical market situation where suppliers compete for the interest of potential hijackers. However, not all platforms allow for interaction between suppliers and potential hijackers, which we elaborate in the next paragraph. We apply the CEP by jointly studying settings where stolen credentials are disseminated and how these illicit products are offered in those settings.

In this study, we cannot directly observe the exchanges between suppliers and potential hijackers, but we observe and analyse how suppliers offer their products. This supply-side analysis is, however, reflective of the choices potential hijackers face when searching for stolen credentials online. From the perspective of the supplier, our analysis shows the outcome of how they decided to offer their product. For potential hijackers searching for stolen credentials online, the different platforms and posts we analyse are nested choice sets related to the two key phases in their search process. They first have to choose a specific platform from which to obtain credentials. Once on a platform, they have to choose between specific posts in which credentials are offered. When searching online, hijackers could iterate through these two phases. If they cannot enter a platform or do not find posts to their liking, they might look for other platforms or posts and repeat their search process. We describe and compare attributes of different online platforms where stolen credentials are offered, how these credentials are offered, and how the offers vary by platform.

Online dissemination on platforms

The focus of the present study is on three different platform types, namely: (1) online discussion forums, (2) online marketplaces, and (3) paste websites. Online discussion forums are rather structured websites with discussions grouped in threads and by topic (Frank, Macdonald, and Monk 2016). A discussion starts when a forum member creates a thread by posing a question or making a statement on a particular topic (Holt 2013). The following discussion revolves around that specific question or statement. Sometimes forums also have designated trade sections (Afroz et al. 2014; Hutchings and Holt 2015). Some forums are dedicated to the underground economy of vulnerabilities and stolen data trade (Frank, Macdonald, and Monk 2016). Examples are carding forums and security forums. Products shared or traded on such forums vary greatly, from stolen personal and financial details to tutorials and vulnerability exploits (Allodi 2017; Samtani, Chinn, and Chen 2015). Research on discussion forums serving the underground economy has largely focused on stolen financial data and threat analysis (Benjamin et al. 2015; Haslebacher, Onaolapo, and Stringhini 2017; Van Hardeveld, Webber, and O'Hara 2016). However, the dissemination of stolen account credentials on discussion forums has received much less attention.

Online marketplaces are aimed at trading goods and services (Kestenbaum 2017). An online marketplace enables vendors to advertise their products to potential customers. Because vendors can operate relatively anonymously – which may decrease trust among buyers – online marketplaces often have reputation systems in place allowing buyers to provide public feedback on the vendor after a transaction (Przepiorka, Norbutas, and Corten 2017). Online underground marketplaces are very similar in structure, but are aimed at trading illegal goods and services. Most online underground markets analysed to date revolve around the illicit trade of drugs (e.g., Dolliver 2015; Kruithof et al. 2016; Przepiorka, Norbutas, and Corten 2017). Nevertheless, underground marketplaces such as Silk Road 2 (now defunct) also had trade sections for virtual products, such as books, software, and data. Moreover, in the case of Silk Road 2, far more transactions occurred in the category 'Counterfeit/data', including data dumps, than in the category 'Drugs' (Dolliver 2015).

Finally, paste websites are websites mainly intended for code sharing. Users of these websites can usually only post plain text. These texts can either be made publicly available or shared among a select group of users. The content on paste websites is not always moderated, which sometimes implies that anybody can post anything (Kelion 2012). It is, therefore, not uncommon for data thieves to publish their stolen credentials on paste websites (High-Tech Bridge 2014; Stone 2015).

Online dissemination through posts

Although stolen data are sometimes disseminated for free, previous research has largely focused on the trade in stolen data. To trade credentials, vendors post advertisements of their credentials on online platforms. In these advertisements, vendors can detail the credentials for sale and include additional information on how they do business, such as the format in which orders should be placed, terms regarding if and how an order will be replaced if the credentials do not work as advertised, or reasons for not contacting the vendor (Afroz et al. 2014; Hutchings and Holt 2015). Vendors sometimes also include information on how they obtained the advertised credentials. Whereas some vendors state they obtained the credentials themselves, others indicate that their credentials were supplied from elsewhere. Prices set for credentials could include a re-sale margin. However, re-selling credentials increases the chance that previous users have flagged security systems of service providers, thus rendering the credentials less valuable if not useless.

In some cases, only some users are allowed to post advertisements. Forum rules could dictate members to have at least a number of posts in their name or a certain status or reputation before being allowed to advertise (Afroz et al. 2014). Alternatively, vendors could be required to pay the website owners for placing an advertisement (Hutchings and Holt 2015). Sometimes advertisement fees are only imposed on those who have not gone through a verification process for vendors. This verification process is one way of trying to minimise the presence of rippers on trade platforms. Rippers post advertisements in which they claim to have something for sale, but do not deliver after payment and instead run off with the money. If there are many rippers present on a platform, the reputation of the platform is undermined and trustworthy vendors might move their business elsewhere and leave the so-called ripper platform (Herley and Florêncio 2010; Holt and Lampke 2010).

Because suppliers can offer their credentials on different types of platforms, potential hijackers have a range of options to choose from, both in terms of platforms to browse and offers to consider. At this point, we assume suppliers try to make their offers as appealing as possible to potential hijackers by anticipating rational choice behaviour from potential hijackers. This assumption reflects a classical economic model where market participants act with bounded rationality (Arthur 1994). That is, they weigh the rewards, costs, and risks of their actions before acting with the limited information they can process. Because little is known about actual behaviour of potential hijackers, we use this assumption merely to structure our data analyses and empirical findings. This approach has also been applied before to examine stolen data markets (Smirnova and Holt 2017). In the next section, we elaborate on how we sampled platforms and posts, and how we structured our data analyses and findings in relation to the rewards, costs and risks for potential account hijackers.

Data and methods

Collecting platforms and posts

Three platforms, all offering stolen account credentials but differing in main purpose, were analysed. The specific discussion forum, marketplace, and paste website analysed were, respectively, Darkode, AlphaBay, and Pastebin. Darkode used to be a notorious invitation-only and password protected hacker forum until it was shut down by the FBI in 2015 (Department of Justice 2015; Moyer 2019). The data from Darkode were obtained from a public website where screenshots of the forum were leaked (Xylitol 2013).[1] Dupont et al. (2017) extensively described this dataset as well as the background of Darkode. The dump of screenshots was structured similar to the structure of the forum. The forum contained several sales sections where members could trade products. For the present study, all 319 screenshots from the sales sections of the forum were analysed. Because some threads encompassed multiple pages and thus multiple screenshots, the 319 screenshots related to 249 unique threads. Account credentials were offered in 32 of these threads. These 32 threads were subsequently coded and used for analysis.

AlphaBay was one of the largest online underground marketplaces with a focus on drug trade until the FBI shut it down in 2017 (Department of Justice 2017). To analyse posts on AlphaBay, we used a dataset composed of 139,773 posts that were scraped in June and July 2013 (Norbutas 2013). Each post was already classified as an advertisement for either a physical or a digital item. As stolen credentials are digital items, only the 36,313 digital items were selected for this study. Table 1 provides an overview of the number of posts listed in each main category on AlphaBay. For the present study, we focused on the subcategory 'Fraud' and within Fraud on the subcategory 'Accounts & Bank Drops'. Within this subcategory, vendors could also categorise their products into several account categories that are outlined in Table 1 (e.g., Amazon, AOL, Bank drops). This subcategory contained 9,041 posts. Most posts containing personalised listings or having tutorials for sale were filtered out with regular expressions. This reduced the sample to be analysed further to 6,756 posts. If an account category contained less than sixty posts, all posts were coded for relevance (i.e., offering account credentials or not). If an account category contained more than sixty posts, at least twenty randomly picked posts were read until at least ten posts offering account credentials were identified. This way, 675 posts were read, from which a total of 243 posts were relevant and used for further analysis.

Pastebin is currently one of the largest paste websites on the internet. Pastebin was intended for sharing plain text, usually source code snippets. However, it is also used for dumping account credentials (High-Tech Bridge 2014; Stone 2015). Pastebin was scraped using Pastebin's scraping API during three weeks in August 2018, four times a day for thirty minutes. This resulted in a sample of 68,359 posts, which translates to an average of 1,627 posts being posted each hour. Because the sample was too large to filter manually for relevance, regular expressions were used to filter out the majority of irrelevant posts.

To construct classification rules for the regular expressions, we used the website psbdmp.ws, which claims to collect all Pastebin posts containing sensitive information. We selected the posts on psbdmp.ws based on their timestamps to ensure these posts were in our scraped sample as well. The psbdmp.ws sample consisted of 366 posts. These posts were all manually coded for relevance. We

Table 1. Number of posts listed in each category on AlphaBay.

Main categories	n	Categories within 'Fraud'	n	Categories within 'Account & Bank drops'	n
Carded Items	655	Accounts & Bank Drops	9,041	Amazon	170
Counterfeit Items	678	CVV & Cards	1,854	AOL	45
Digital Products	7,857	Dumps	558	Bank Drops	2,457
Drugs & Chemicals	83	Personal Information & Scans	2,144	Deezer	59
Fraud	15,656	Other	2,059	Ebay	126
Guides & Tutorials	6,623			Google	74
Jewels & Gold	3			Hotmail & Outlook	55
Other Listings	977			Netflix	91
Security & Hosting	318			Origin	43
Services	2,110			Porn	537
Software & Malware	1,351			Spotify	75
Weapons	2			Steam	49
				TV & Cable Providers	148
				Uber	79
				Uplay	42
				Yahoo	48
				Other	4,943

applied the classification rules constructed from this sample to all 68,359 posts, which resulted in 5,085 potentially relevant posts. Because this sample was still very large and contained many false positives (i.e., irrelevant posts considered relevant by the classification rules), we read through 2,673 posts that were randomly picked from this sample. Eventually, this left us with 188 posts offering stolen account credentials on Pastebin.

Categorising account sources

When reading posts, we noted that offered accounts span a great number of sources (i.e., organisations and websites servicing the accounts). Sources were categorised into the following nine source types: Entertainment, Webshop, Adult, Financial, Game, Social, Telecom, Other, and Unknown. If credentials from multiple source types were offered as one package, we coded the dominant source type of the majority of credentials. If there was no dominant source type or the source type did not fit into one of the other categories, the post was classified as 'Other'. However, if different accounts were offered for different prices in the same advertisement, we coded them separately, which resulted in disaggregating posts to the level of the source type offered. The list of source types and common examples of these source types are presented in Table 2, along with how many posts offered accounts from the corresponding source types.

The most common source types were financial institutions and entertainment services. AlphaBay posts always specified the source of the accounts. In contrast, the specific source type was often not mentioned on Darkode and Pastebin. Instead, Darkode posts often contained information on the type of organisation the accounts belonged to, or just how popular the website was. Popularity of a website was suggested by the rank of that website based on website traffic. For instance, one member titled his (or her) advertisement: '*Alexa Rank 10k. US rank: 9k. Niche: News site. Open bid*'. Darkode members were also largely prohibited to sell stolen financial information. If no source on Pastebin was specified, the post only contained one or multiple lists with usernames or e-mail addresses and passwords. Account dumps like these almost never contained financial information. Conversely, all posts on Pastebin offering financial information were more similar to advertisements on AlphaBay: they stated a specific source, asked a price, and mentioned a vendor.

Conceptualisation and coding scheme

The goal of the present descriptive study is to gain a better understanding of the illicit dissemination of stolen account credentials. More specifically, we aim to provide insight into how stolen credentials are offered on different online platforms. Although platform and post attributes can be coded in various ways, such as by the colour of a webpage or the length of a post, we adopted a rational choice approach to guide our coding scheme. Assuming that potential hijackers weigh the rewards, costs, and risks of obtaining account credentials, we categorised the scraped data along these three factors.

Table 2. Number of posts coded by source type and platform.

Source type	Examples	Darkode	Pastebin	AlphaBay
Entertainment	Netflix, Spotify	5	31	67
Financial	Paypal, Suntrust	0	65	38
Webshop	Ebay, Amazon	3	1	49
Social	Skype, Gmail	4	3	22
Adult	Brazzers, dating	1	5	20
Game	Steam, Uplay	0	13	12
Telecom	AT&T, Comcast	0	0	14
Unknown		14	48	0
Other		5	22	21
Total		*32*	*188*	*243*

How rewarding browsing platforms and engaging in transactions is, depends in part on the motivation and intent of account hijackers. Whereas some hijackers might look for accounts of a specific company, others might look for e-mail accounts or just any pair of working account credentials (and try those on other types of accounts). However, obtaining more account credentials and more additional account information for the same price will generally be more rewarding. Therefore, for each post, we coded how many account credentials and additional information were offered.

Account hijackers potentially face costs in terms of time and money. Stolen credentials are not widely advertised due to their illicit nature. Therefore, finding and browsing platforms where such credentials are offered could take quite some time. If account credentials have a price tag, the price will likely also go into the equation, as money is a cost in all sorts of transactions. Therefore, search costs and financial costs were coded as cost attributes. More specifically, search costs translated to reachability and accessibility of platforms, and what search features are in place. Financial costs translated to the information found on the price of products.

We note here that to code the price, we calculated the price per account, if multiple accounts were offered as a package deal. Because bidding was possible on Darkode, we coded the highest price mentioned in a thread and calculated the price per account. Although it is likely that bidding also took place in private communications rather than on the public forum, we had no way of establishing how much money was offered in private.

Finally, account hijackers risk at least ripper and law enforcement activity when searching for stolen credentials. Potential hijackers need to trust that credentials will be as good as advertised and the supplier does not rip them off. This results in a trust problem on markets because hijackers and suppliers operate in anonymous environments (Przepiorka, Norbutas, and Corten 2017). Hijackers thus do not know with whom they are dealing. Platforms could try to mitigate the risk of both rippers and law enforcement, whereas suppliers could specifically attempt to appear honest. The risk of dealing with rippers could partly be alleviated by platforms through admission and verification procedures (Dupont et al. 2017; Hutchings and Holt 2015). The risk of detection by law enforcement is relevant for both platforms and potential hijackers. As demonstrated by the cases of the underground online markets AlphaBay and Hansa, platforms facilitating illegal activities can be shut down by law enforcement (Department of Justice 2015, 2017). Platforms might, therefore, apply measures to decrease the likelihood of law enforcement presence, such as access control.

Risk attributes coded specifically relating to platforms were measures aimed at anonymization and preventing rip-offs (Yip, Webber, and Shadbolt 2013). As for posts, to minimise distrust or suspicion, suppliers could state in their posts that they provide customer services, such as replacements for invalid credentials (Holt, Chua, and Smirnova 2013). If potential hijackers would receive invalid credentials, they would not risk having paid for credentials that do not work. In a similar vein, offering customer service lines or support for hijackers encountering issues they cannot solve themselves decreases the chance of paying for credentials that cannot be used. Customer services are, therefore, coded as risk attributes relating to platforms.

Before continuing to our results, we provide two cautions for our readers. First, because we could not browse AlphaBay and Darkode ourselves, some information might be lacking. Nevertheless, these scrapes do provide information about the ease with which these platforms could be reached and searched, how risks were mitigated by platforms and vendors, and what information on products was available. Second, we decided to categorise the data in relation to the potential rewards, costs, and risks for potential account hijackers, because we assume the platforms operate as markets for illegal goods and services and the actors in these markets behave with bounded rationality. However, we cannot use our scheme to make inferences about the actual decision-making process of potential hijackers nor of the suppliers of stolen credentials. We provide directions for future research to examine the actual decision-making processes at the end of our paper. In the next section, we present our results. We mainly describe platform attributes and we use descriptive statistics for post attributes.

Results

Platform attributes

Table 3 presents an overview of variation in attributes among the three platforms. Reward attributes were hardly present on platforms. None of the platforms provided indicators of what was offered in posts, except for AlphaBay providing a measure indicating how much of a product the supplier had in stock. Rewards of searching for and browsing platforms can thus only be determined by reading posts.

Financial costs were clearly indicated on AlphaBay. The price is stated as metadata on this platform, whereas prices on Darkode and Pastebin are only visible inside posts. Regarding search costs, Pastebin is much more accessible than the other platforms. It can be accessed without having to register and, as we noted during scraping, thousands of posts are publicly posted every day. However, neither we nor potential hijackers can establish easily if private posts offer account credentials more often than public posts. In addition, no post categories existed and posts were only sorted by the time they were posted. AlphaBay was the only platform with a search menu in which the product type could be specified. Darkode was largely structured by social hierarchy. Some parts of the forum could only be accessed by higher ranking members. Each level had a marketplace section, however. To exemplify, subforums for Level 0, 1, and 2 members all had marketplaces. Level 1 members could access the level 0 and 1 marketplace, but not the level 2 marketplace. Restricting views from (new) users makes it harder for hijackers to find posts offering credentials, but minimises the risk of law enforcement engagement. Higher search costs for potential hijackers thus imply a lower risk of being caught by law enforcement.

AlphaBay and Darkode further decrease the risk of being ripped-off by applying measures to rate vendor reliability and product quality. Members can rate other members, resulting in different types of public member ranks. Furthermore, members can post comments and provide feedback on posts which are subsequently published below that post. Pastebin did not provide the option of commenting on posts. Moreover, anyone could post anything on Pastebin, which greatly increases the likelihood of dealing with rippers.

Post attributes

Whereas the previous section describes general post attributes, this section details the variation in attributes of posts in which account credentials were offered. A total of 243, 32, and 188 posts were analysed from AlphaBay, Darkode, and Pastebin respectively. First, we describe what variation we noted in reward attributes. Next, we elaborate on prices as a cost attribute and relate this to several reward attributes. We conclude the results section by describing several risk attributes noted in posts.

Rewards

Reward attributes coded relate to what is offered and how much is offered. We coded if credentials were visible, how much credentials were offered and what additional information on accounts and account holders was offered. Credentials were immediately visible in 12, 6, and 117 posts on respectively AlphaBay (4.9%), Darkode (18.8%), and Pastebin (62.2%). Because AlphaBay and the Darkode marketplace were dedicated to trade, it makes sense that very few credentials were immediately visible to potential buyers. Credentials visible on those platforms mainly served to clarify what kind of information hijackers would receive (e.g., a username or e-mail address, password, name, gender, etc.).

Posts did not always specify how many unique account credentials were offered. AlphaBay posts were least often explicit about the number of credentials on offer with less than ten per cent (23 out of 243) containing an exact number of accounts. Posts explicitly specifying the number of account credentials for sale allowed buyers to buy 100,000 account credentials or more per transaction. Posts

Table 3. Platform attributes.

Attribute category	Attribute	AlphaBay	Darkode	Pastebin
Costs	*Reachability*	Tor Hidden Service, password protected	Password protected	Everyone can access
	Accessibility	Vendors can hide ads for new or unestablished users	Only accepted members could access trade sections	Post can be kept private, but default is public. Expiration date of posts
	Search features	Extensive search menu, search results can be sorted, product categories	Search bar, posts sorted by social hierarchy	Search bar, posts only sorted by the time of posting.
	Price of products	Price and payment type as metadata	Only in thread.	Only in posts
Risks	*Anonymity*	Nickname required. Unknown if members had a profile page	Nickname, profile page with e.g., registration date, posts posted, contact details, interests	If not ‘Guest’: nickname, profile page with e.g., registration date, posts posted
	Vendor reliability	Vendor level, trust level	Social hierarchy level, karma score	Registered or unregistered
	Product quality	Feedback: good, bad, or neutral. Date of posting.	Replies in thread and number of views. Date of posting	No commenting possible. Number of views. Date of posting
Rewards	*Number of accounts*	Quantity left	Only in thread	Only in posts
	Additional information	Only in posts	Only in posts	Only in posts

without an exact number of accounts were often advertised like: ‘*Selling Amazon Account with Credit Card attached*’, or: ‘*All accounts come with Lifetime Warranty!!! so if your login stops working I will replace the account for you*.’ Therefore, we assume that, in the majority of cases, account hijackers could obtain a single account (i.e., one pair of credentials) per transaction. On Pastebin, 124 posts specified how many credentials were offered. Half of the posts in which the number of credentials offered was specified (51.6%) offered credentials of less than 20 accounts. However, a small fraction of those posts (11.2%) contained rather long lists of more than 500 accounts credentials. Whereas posts on AlphaBay and Pastebin thus seem to offer credentials for just one account or tens to hundreds of accounts, credentials on Darkode were mainly offered in much larger quantities, namely ranging from 2,300 to 4.8 million accounts.

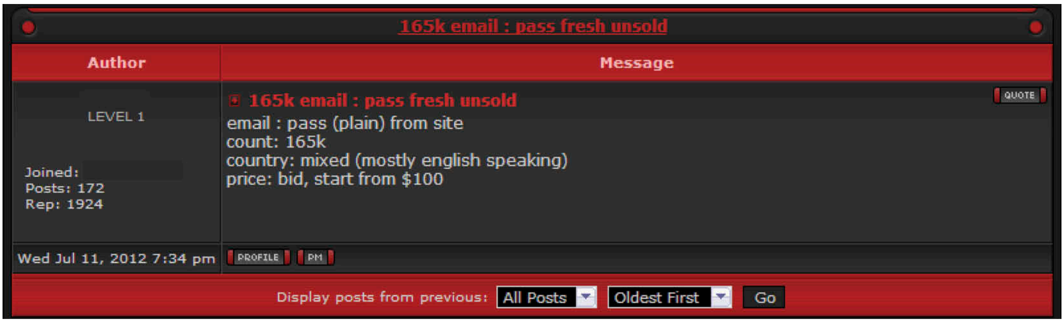
Coding additional information on accounts and account holders was largely a bottom-up process. Following Franklin et al. (2007), we coded at least if the name, address, phone number, and social security number of account holders were provided. While reading, we noted what other additional information was provided. As will be explained at the end of this paragraph, types of additional information barely noted were not included in our comparisons. Although credentials leaked on Pastebin are immediately visible, these credentials are usually not accompanied by any other account information, such as the account type (e.g., standard or premium), when the account was last used, and information on the account holder (e.g., name and address). Posts on Darkode and AlphaBay provided more additional information to potential hijackers. Table 4 demonstrates how oftendifferent types of information on accounts and account holders were noted in the full sample of posts offering credentials. In general, little additional information was provided on accounts or account holders, except for the account balance. Account balance here is rather broadly defined. It refers to any type of balance that could indicate how valuable an account is, such as points collected through gaming or shopping, but also to the amount of feedback account holders received, gift card values stored in accounts, or simply the balance on financial accounts. Vendors on AlphaBay did not always include information on the balance of financial accounts, which could imply that the accounts had no balance or the vendor did not know the balance. Either way, in those cases, potential hijackers would thus buy a financial account without knowing if and how much money was associated with the account. Although we also coded information provided to bypass two-factor authentication, gender, date of birth, and social security numbers of targets, these types of information were less common than the additional information in Table 4. The general lack of additional information on accounts or account holders implies that potential hijackers usually have to decide on a transaction mainly by considering the account source, the number of accounts, and the price.

Costs

The cost attribute coded for posts was the price asked for credentials. Prices were less common on Pastebin, because of the large number of posts with visible credentials on this platform. Only advertisements about financial accounts on Pastebin (34% of the posts) included a price. On Darkode, nearly all posts stated that account credentials were for sale. However, instead of stating

Table 4. Additional information provided on accounts and account holders.

	N	Name	Address	Phone	Points	Account type	Linked accounts	Browser	Last activity
Financial	103	9	11	5	86	6	6	5	7
Entertainment	103	1	*0*	1	*0*	54	1	*0*	*0*
Webshop	53	15	19	5	34	5	11	8	20
Social	36	8	6	10	2	*0*	8	4	*0*
Adult	26	*0*	1	*0*	1	14	*0*	*0*	*0*
Game	25	*0*	*0*	*0*	13	2	*0*	*0*	*0*
Telecom	14	1	2	3	1	2	*0*	*0*	*0*
Unknown	62	6	7	4	2	2	*0*	4	1
Other	41	8	7	8	8	9	12	2	*0*
Total	463	48	53	36	146	94	38	23	28



165k email : pass fresh unsold

Author | Message

[redacted]
LEVEL 1

Joined: [redacted]
Posts: 172
Rep: 1924

165k email : pass fresh unsold
email : pass (plain) from site
count: 165k
country: mixed (mostly english speaking)
price: bid, start from $100

Wed Jul 11, 2012 7:34 pm

Display posts from previous: All Posts Oldest First Go

Figure 1. Darkode member offering account credentials.

a fixed price, it was common to place a starting bid or merely state that credentials were sold to the highest bidder, as illustrated in Figure 1. Readers could subsequently place their bids in the thread or send a personal message (‘*pm*’) to the member starting the thread. Although large packages of tens or hundreds of thousands of credentials were offered, bids often started at less than 400 USD and sometimes even at less than 100 USD. This boils down to a price of less than a dollar cent per credential. Because the majority of credentials posted on Pastebin were freely accessible and the Darkode sample only contained 32 posts, the remainder of this paragraph elaborates on prices stated in the 243 analysed posts on AlphaBay.

AlphaBay did not allow bidding, so all credentials offered had a fixed price as specified by the vendor. Table 5 provides an overview of the average price per account sorted by source type. Financial accounts were most expensive (mean asking price = 107 USD), followed by webshop accounts (mean = 32 USD). Financial accounts were often advertised with information on financial balance, which could explain the higher asking price. Regarding webshop accounts, these accounts are potentially easier to monetise than other types of accounts, as these accounts are already used for doing business. In addition, as opposed to other types of accounts, webshop accounts were sometimes offered together with financial accounts, which should make it even easier to monetise the webshop accounts. Social and game accounts appeared to be least valuable (respective means are both 2 USD). Thirty posts specified no price for the advertised account credentials. In some posts, the price was set at 0 USD. However, a zero-dollar price did not imply that the credentials advertised were for free, because vendors explicitly stated in their posts that accounts were for sale: ‘*purchase options are shown bellow …* ’, or ‘*Buy with confidence*’.

Nineteen posts contained a price list in which the price depended on, for instance, the number of months an account was guaranteed to work (for entertainment accounts), how many accounts were sold (for packages of e-mail accounts), or the balance on the account (financial accounts or gift card balance on webshop accounts). One vendor stated in his (or her) post: ‘*Minimum 10,000 Avios Points ~ $2.50, Minimum 20,000 Avios Points ~ $5.00, Minimum 40,000 Avios Points ~ $8.00, Minimum 80,000 Avios Points ~ $14.00*’.

Table 5. Average price in USD per account by organisation type on AlphaBay.

Source type	N_{total}	n_{single}	*Mean*	Median	Min	Max
Financial	76	35	107.22	33	0.75	1400.00
Webshop	41	37	31.85	7.00	0.99	217.80
Telecom	18	14	9.93	10.00	1.59	25.00
Adult	17	17	5.37	4.99	0.0001	15.99
Entertainment	62	60	3.12	1.99	0.05	25.00
Social	26	20	2.21	0.99	$1*10^{-6}$	15.00
Game	12	12	2.11	2.00	0.1	5
Other	23	18	21.56	5.94	0.003	175.00

Note. N_{total} = all posts split out. N_{single} = all posts, no subposts included.

Posts offering financial accounts most often contained a price list. Prices in those lists always depended on the balance of the financial account. The higher the balance, the more expensive the account, similar to the previous example in which the price depended on the number of points. Splitting the eleven posts offering financial accounts with a price list into a different subpost for each price resulted in a total of 76 financial subposts. As illustrated in Table 5, the prices of these subposts ranged from 0.75 USD to 750 USD, with one outlier of 1,400 USD. The balances ranged from 20 USD up to 250,000 USD.

Although posts with a price list on AlphaBay differed in what they offered, all consistently offered non-cumulative quantity discounts, i.e., the more accounts or the more valuable accounts you buy, the more discount you get. We found this type of discount on all three platforms analysed. The graphs in Figure 2 exemplify typical non-cumulative quantity discounts on financial accounts offered on Pastebin. A few posts on Pastebin also offered e-mail account credentials for sale in bulk, resulting in very cheap prices per account. For instance, a package of 1,000 e-mail credentials was offered for 50 USD, which means one account costs five dollar cents. Members on Darkode offered their packages of account credentials in even larger sizes and their prices were relatively lower. The majority of credentials (n = 29; 90.6%) on Darkode was cheaper than one dollar cent per account.

Finally, we examined the relationship between additional information on accounts and account holders, and the price of accounts for all posts on AlphaBay. Posts offering financial accounts were not included, because those accounts were generally far more expensive than accounts from other types of sources and would therefore greatly affect the relationships to be compared. Table 6 reveals higher asking prices for advertisements providing additional information on accounts and account holders. Vendors providing at least one of the listed types of additional information had a higher asking price than vendors who did not provide such information at all ($U = 3258.50$, $p < .001$, $r = .27$). This suggests that more rewarding items are costlier to obtain.

Risks

Coding risk attributes was, similar to coding additional information on accounts and account holders, largely a bottom-up process. While reading, we noted customer services such as customer service lines and free replacements (Holt, Chua, and Smirnova 2013). These services are aimed at improving customer satisfaction and could, therefore, affect the perceived risk of doing a transaction. We also noted terms and conditions (i.e., transaction rules) posed by vendors restricting what buyers could do after a bad transaction (e.g., buying invalid credentials). Because such rules could make doing business seem more risky, they were coded as well.

When credentials on Pastebin were visible to anyone, no transaction rules were specified. Advertisements for financial account credentials on Pastebin and posts on AlphaBay and Darkode

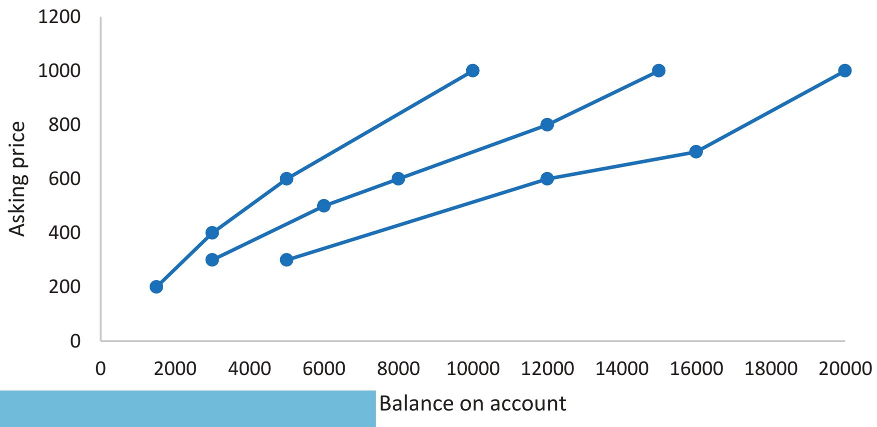


Figure 2. Non-cumulative quantity discounts on financial accounts offered in three Pastebin posts.

Table 6. Price of credentials on AlphaBay when additional information was (not) included.

		Information included		Information not included	
	N	*M (SD)*	Median	*M (SD)*	Median
Name	18	34.83 (62.64)	10.35	10.65 (24.68)	2.95
Address	22	32.69 (56.96)	10.35	10.37 (24.77)	2.67
Phone	25	14.79 (36.53)	2.99	12.56 (29.81)	3.00
Points	44	29.52 (46.11)	9.00	8.10 (22.61)	2.57
Account type	59	10.07 (24.76)	3.39	14.01 (32.82)	2.85
Linked accounts	31	16.60 (33.84)	4.00	12.15 (30.07)	2.99
Browser	8	68.31 (84.78)	17.5	10.52 (24.05)	2.99
Last activity	15	59.09 (76.30)	7.00	9.07 (19.51)	2.99

sometimes did stipulate transaction rules and what customer services were offered to buyers. The most common rules and services are reported in Figure 3. Only posts in which credentials were sold, and thus not freely disseminated, are included in this comparison. As can be seen in this table, the rules and services coded were mainly specified in posts on AlphaBay.

The most common services mentioned were warranties and refunds or replacements. Interestingly, warranties on sold accounts were especially prominent in posts on Pastebin. These warranties mainly applied to the balance on financial accounts. Vendors claimed, for instance, that they would guarantee that the money on their accounts would not be stolen by anyone nor would it be returned to another account (if the money originated from another account; i.e., no charge backs): '*all transactions are secured, zero theft and no charge back. 100% SECURED*'. Because financial accounts are sometimes advertised as having quite a lot of money on their balance and they are rather expensive, compared to other types of accounts, buyers risk losing a lot of money if the vendor turns out to be a ripper. Therefore, it makes sense that vendors try to reassure potential buyers by claiming to provide warranties. However, although warranties were less common on AlphaBay (n = 21), when warranties were stated, they more often applied to entertainment and adult accounts (n = 15) than

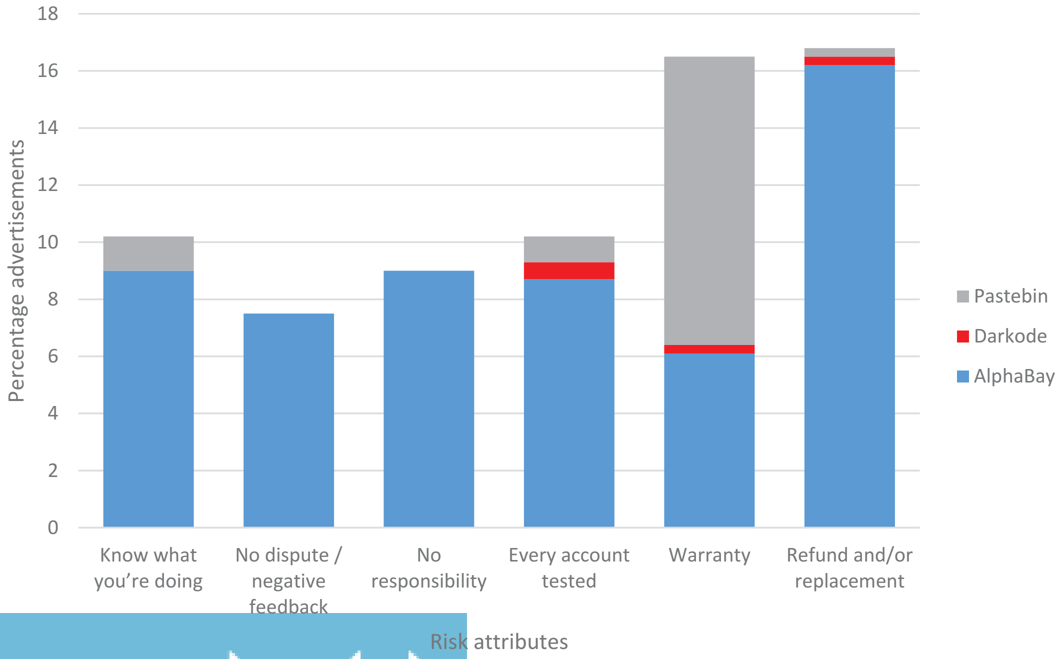


Figure 3. Percentage of advertisements mentioning the most common rules and services.

to financial accounts (n = 2). Warranties on entertainment and adult accounts referred to guarantees from vendors that the account would work, sometimes for a minimum period of time.

Offering replacements or refunds for invalid credentials also serves to reduce the risk potential hijackers face when spending money on account credentials. Statements on replacements or refunds were most common on AlphaBay. Replacements (n = 49) were far more common than refunds (n = 15). Although replacements and refunds were offered as services, nineteen posts explicitly stated that they would never give a refund. One vendor offered no refunds or replacements at all. In a similar vein, some vendors tested their accounts before providing them (n = 30), whereas others did not (n = 10). The following example nicely summarises common rules and services posed by vendors on AlphaBay:

> Buy ONLY if you know how to use them! I'm not responsible for your movements, cash out method failure, security questions etc.! Replacement ONLY if the login details are wrong. Buyer who leave negative feedback without any good reason will be ignored in future. When you purchase from my listing you agree with the terms.

Because AlphaBay had a reputation system implemented, negative feedback could damage vendors' businesses. Therefore, some vendors threatened to blacklist buyers in the future if they would leave negative feedback after a transaction. This rule was typical for AlphaBay vendors, as it was not noted on the other platforms. In contrast, typical for Darkode members were remarks about the format of passwords. Some offered unencrypted passwords that could be used immediately, whereas others stated that buyers would have to crack passwords before those could be used (n = 12; 37.5%).

Discussion

The present descriptive study was aimed at providing insight into platforms where stolen account credentials are disseminated and how offers on credentials vary by type of platform. Previous research mainly focused on stolen financial data, such as credit card data, and largely neglected stolen account information. However, account hijacking could be more damaging than the abuse of financial data and affects the full spectrum of accounts instead of merely financial accounts. In our research, we took a criminal event perspective by jointly studying the crime settings and the illicitly disseminated products.

The platforms compared were a paste website, an underground market, and a discussion forum. The paste website was most easy to reach and access, and most credentials offered there were freely disseminated. The market and forum were harder to reach and access. Credentials on these platforms were usually sold. On the market, credentials were mainly sold per piece, whereas on the forum, credentials were often sold in bulk. The most expensive types of accounts on the market were financial and webshop accounts. The forum also substantially facilitated interaction between suppliers and potential hijackers, more so than the market and in contrast to the paste website. Due to greater interaction on the forum, bidding was common on this platform. On all three platforms, non-cumulative quantity discounts were offered. Finally, warranties, refunds, and replacements were the most common customer services offered. Warranty claims were especially prominent on the paste website where no reputation system was in place and the risk of doing business is rather high. Conversely, suppliers threatened to blacklist buyers – if they left negative feedback – on the market, which is a platform with a clear reputation system.

Although this study systematically examined the illicit act of disseminating stolen credentials online, it is an explorative study with several limitations. For instance, it was not always clear if the offered credentials had in fact been stolen. Some suppliers stated that their accounts were *created* rather than hacked (i.e., stolen). Reasons to offer created accounts include not risking that the account would close down or that the password would change. Although implied, in about a third of the cases (32.6%) we analysed it was stated explicitly that the credentials were stolen.

Other limitations relate to the sampling scheme. For instance, we lacked information about AlphaBay and Darkode because we did not scrape these platforms ourselves and the platforms did not exist anymore when conducting our analyses. This resulted in missing data when coding platform attributes, such as the presence of profile pages on AlphaBay. In addition, it is likely that deals on Darkode were made through private communications instead of public posts. Therefore, we cannot be sure if and when the asking price was also the final selling price. Regarding Pastebin posts, we based our filtering method on a second website claiming to collect all sensitive information dumped on Pastebin. Although it seemed to sample a large number of these dumps, including posts we did not consider as such, this sampling method could have resulted in false negatives (i.e., filtering out posts containing account credentials). Despite these limitations, this is the first study we know of to have systematically analysed platform and post attributes in the context of stolen account credentials.

Policy implications and directions for future research

Several agents could intervene in the act of illicitly disseminating stolen credentials and subsequent exploitation of those credentials. In this section, we discuss two of these agents, namely law enforcement and organisations servicing online accounts. Because of the widespread use of anonymising software by actors on illicit online platforms, tracking and tracing these actors is challenging for law enforcement. Therefore, countermeasures deployed by law enforcement are likely best directed at platforms hosting the illicit content. At the time of writing, law enforcement agencies from different countries have already cooperated to take down several large illicit online marketplaces, such as AlphaBay, Hansa market, and Wall Street Market (Ewing 2019). While several arrests have resulted from taking down these websites, it is suggested that these types of law enforcement activity have no lasting effect on the ecosystem of illicit online markets (Greenberg 2019). After some markets have been shut down, other markets pop up and business goes on as usual.

Although organisations servicing accounts (e.g., Google and Netflix) have no power to take down online platforms where their accounts are traded, they can make those accounts less valuable to potential hijackers. Our findings demonstrate that accounts with additional information on accounts or account holders were generally sold for higher asking prices than accounts without such information. We also noted that, in general, little additional information was offered. This could reflect the increased effort suppliers had to make to obtain additional information. It could also imply that a username-password combination on its own is less valuable. Indeed, more organisations nowadays provide the option of two factor authentication (Griffith 2019). This security measure requires hijackers to enter additional information during the login process besides a correct username-password combination. Because taking down the ecosystem of illicit online platforms and apprehending potential hijackers is challenging for law enforcement, decreasing the value of stolen credentials by increasing account security may be a more fruitful approach.

Because little scientific research has been conducted on the topic of stolen credentials and account hijacking, there are many avenues for future research. The CEP encourages researchers to consider the bigger picture of the illicit acts of disseminating and exploiting stolen credentials (Meier, Kennedy, and Sacco 2001). So far, we have only considered platforms and posts disseminating credentials. As stated previously, it appears that law enforcement activity does not have a lasting effect on the illicit trade of credentials. However, as far as we know, there is no scientific evidence of the (lack of) effects. Therefore, our first suggestion for future research is to systematically measure the effects of law enforcement activity on the ecosystem. This could guide law enforcement in adjusting their countermeasures or justify maintaining their current tactics.

Our second suggestion relates to our assumption that hijackers act with bounded rationality. Because little is known about their motivations and actual decision-making process, we encourage future research to test the validity of this rationality assumption. One way to test hypotheses on their motivations and decision-making process is by deploying a honeypot design. Honeypots are decoy computer systems mimicking real computer systems but designed to be attacked (Bringer, Chelmecki, and Fujinoki 2012). Because honeypots look authentic and valuable, attackers do not (always) realise they are attacking a honeypot. For instance, Onaolapo, Mariconti, and Stringhini (2016; Villalva, Onaolapo, Stringhini, & Musolesi, 2018) deployed honey e-mail accounts to systematically leak account credentials and observe hijackers' behaviours inside accounts. Furthermore, Maimon et al. (2014), tested decision-making theories by examining the effect of different types of warning banners in computer systems on hackers' persistence. These studies also demonstrate that honeypot decoys are a good way to observe criminal choice behaviour as it is unfolding, a hitherto almost completely unexplored area of research.

Note

1. http://darkode.cybercrime-tracker.net/.

Acknowledgments

We thank the anonymous reviewers and editor for their helpful comments on an earlier draft and Lukas Norbutas for prematurely disclosing his dataset so we could analyse one additional platform.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the Dutch Research Council (NWO) [Research Talent grant no. 406.17.562].

Notes on contributors

Renushka Madarie is a PhD student at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and Utrecht University. Renushka has a background in psychology and criminology. Her research interests include illicit online markets and cybercriminal behaviour.

Stijn Ruiter, PhD, is Senior Researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and Professor at the Department of Sociology of Utrecht University. His main research interests include the study of spatiotemporal patterns in crime and offender decision-making in both offline and online environments.

Wouter Steenbeek, PhD, is a researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). Most of his work is on the 'geography of crime': describing spatial and temporal variations in crime and explaining these variations as a function of the characteristics of places and how offenders, targets and guardians use their spatial environment over daily and weekly time cycles.

Edward Kleemans is Full Professor (Serious and Organized Crime and Criminal Justice) at the VU School of Criminology, Faculty of Law, Vrije Universiteit Amsterdam, the Netherlands.

References

Afroz, S., A. C. Islam, A. Stolerman, R. Greenstadt, and D. McCoy. 2014. "Doppelgänger Finder: Taking Stylometry to the Underground." Paper presented at the 2014 IEEE Symposium on Security and Privacy, San Jose, CA, USA.

Allodi, L. 2017. "Economic Factors of Vulnerability Trade and Exploitation." Paper presented at the Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA.

Anderson, A. L., and R. F. Meier. 2004. "Interactions and the Criminal Event Perspective." *Journal of Contemporary Criminal Justice* 20 (4): 416–440. doi:10.1177/1043986204269383.

Arthur, W. B. 1994. "Inductive Reasoning and Bounded Rationality." *The American Economic Review* 84 (2): 406–411.

Benjamin, V., W. Li, T. Holt, and H. Chen. 2015. “Exploring Threats and Vulnerabilities in Hacker Web: Forums, IRC and Carding Shops.” Paper presented at the IEEE International Conference on Intelligence and Security Informatics, Baltimore, MD.

Bringer, M. L., C. A. Chelmecki, and H. Fujinoki. 2012. “A Survey: Recent Advances and Future Trends in Honeypot Research.” *International Journal of Computer Network and Information Security* 4 (10): 63. doi:10.5815/ijcnis.2012.10.07.

Bursztein, E., B. Benko, D. Margolis, T. Pietraszek, A. Archer, A. Aquino, … S. Savage (2014). “Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild.” Paper presented at the Internet Measurement Conference (IMC), Vancouver, BC, Canada.

Das, A., J. Bonneau, M. Caesar, N. Borisov, and X. Wang 2014. “The Tangled Web of Password Reuse.” Paper presented at the Symposium on Network and Distributed System Security (NDSS), San Diego, CA, USA.

Department of Justice. 2015. “Major Computer Hacking Forum Dismantled [Press release].” https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled

Department of Justice. 2017. “AlphaBay, the Largest Online ‘dark Market,’ Shut down [Press release].” https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

Detrixhe, J. 2018. “Hackers Account for 90% of Login Attempts at Online Retailers.” *Quartz*, July 18. https://qz.com/1329961/hackers-account-for-90-of-login-attempts-at-online-retailers/

Dolliver, D. S. 2015. “Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel.” *International Journal of Drug Policy* 26 (11): 1113–1123. doi:10.1016/j.drugpo.2015.01.008.

Dupont, B., A.-M. Côté, J.-I. Boutin, and J. Fernandez. 2017. “Darkode: Recruitment Patterns and Transactional Features of ‘The Most Dangerous Cybercrime Forum in the world’.” *American Behavioral Scientist* 61 (11): 1219–1243. doi:10.1177/0002764217734263.

Ewing, J. 2019. “Hunt for Operators of Illicit Marketplace Leads to Arrests in Germany.” *The New York Times*, May 3. https://www.nytimes3xbfgragh.onion/2019/05/03/business/germany-wall-street-market-drugs.html

Frank, R., M. Macdonald, and B. Monk (2016). “Location, Location, Location: Mapping Potential Canadian Targets in Online Hacker Discussion Forums.” Paper presented at the European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden.

Franklin, J., A. Perrig, V. Paxson, and S. Savage 2007. “An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants.” Paper presented at the Conference on Computer and Communications Security, New York, NY.

Golgowski, N. 2017. “The Most Common Passwords In 2016 Are Truly Terrible.” *HuffPost*, January 18. https://www.huffingtonpost.com/entry/2016-most-common-passwords_us_587f9663e4b0c147f0bc299d

Greenberg, A. “Feds Dismantled the Dark-Web Drug Trade—But It’s Already Rebuilding.” https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/

Griffith, E. 2019. “Two-Factor Authentication: Who Has It and How to Set It Up.” https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up

Grommon, E., and J. Rydberg. 2014. “Elaborating the Correlates of Firearm Injury Severity: Combining Criminological and Public Health Concerns.” *Victims & Offenders* 10 (3): 318–340. doi:10.1080/15564886.2014.952472.

Haslebacher, A., J. Onaolapo, and G. Stringhini 2017. “All Your Cards are Belong to Us: Understanding Online Carding Forums.” Paper presented at the 2017 APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, USA.

Herley, C., and D. Florêncio. 2010. “Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy.” In *Economics of Information Security and Privacy*, edited by T. Moore, D. J. Pym, and C. Ioannidis, 33–53. Boston, MA: Springer.

High-Tech Bridge. 2014. “300,000 Compromised Accounts Available on Pastebin: Just the Tip of Cybercrime Iceberg.” https://www.htbridge.com/news/300_000_compromised_accounts_available_on_pastebin.html

Holt, T. J. 2013. “Exploring the Social Organisation and Structure of Stolen Data Markets.” *Global Crime* 14 (2–3): 155–174. doi:10.1080/17440572.2013.787925.

Holt, T. J., and E. Lampke. 2010. “Exploring Stolen Data Markets Online: Products and Market Forces.” *Criminal Justice Studies* 23 (1): 33–50. doi:10.1080/14786011003634415.

Holt, T. J., O. Smirnova, and Y. T. Chua. 2016a. “Exploring and Estimating The Revenues and Profits Of Participants in Stolen Data Markets.” *Deviant Behavior* 37 (4): 353–367. doi: 10.1080/01639625.2015.1026766.

Holt, T. J., Y.-T. Chua, and O. Smirnova (2013). “An Exploration of the Factors Affecting the Advertised Price for Stolen Data.” Paper presented at the eCrime Researchers Summit 2013, San Francisco, CA, USA.

Holt, T. J., O. Smirnova, and Y. T. Chua. 2016b. “The Marketing and Sales of Stolen Data.” In *Data Thieves in Action. Palgrave Studies in Cybercrime and Cybersecurity*, 19–43. New York, NY: Palgrave Macmillan.

Hutchings, A., and T. J. Holt. 2015. “A Crime Script Analysis of the Online Stolen Data Market.” *British Journal of Criminology* 55 (3): 596–614. doi:10.1093/bjc/azu106.

Kelion, L. 2012. “Pastebin: Running the Site Where Hackers Publicise Their Attacks.” *BBC*, April 2. https://www.bbc.com/news/technology-17524822

Kestenbaum, R. (2017). “What Are Online Marketplaces And What Is Their Future?” https://www.forbes.com/sites/richardkestenbaum/2017/04/26/what-are-online-marketplaces-and-what-is-their-future/

Kigerl, A. 2018. “Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories.” *Social Science Computer Review* 36 (5): 591–609. doi:10.1177/0894439317730296.

Kruithof, K., J. Aldridge, D. Décary-Hétu, M. Sim, E. Dujso, and S. Hoorens. 2016. *Internet-facilitated Drugs Trade. An Analysis of the Size, Scope and the Role of the Netherlands*. Retrieved from Santa Monica, Calif. and Cambridge, UK.

Maimon, D., M. Alper, B. Sobesto, and M. Cukier. 2014. “Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System.” *Criminology* 52 (1): 33–59. doi:10.1111/1745-9125.12028.

Meier, R. F., L. W. Kennedy, and V. F. Sacco. 2001. “Crime and the Criminal Event Perspective.” In *The Process and Structure of Srime: Criminal Events and Crime Analysis*, edited by R. F. Meier, L. W. Kennedy, and V. F. Sacco, 1–28. Vol. 9. NJ: Transaction Publishers.

Mell, A. (2012). “Reputation in the Market for Stolen Data (Discussion Series paper).” Oxford, England: Department of Economics, University of Oxford.

Motoyama, M., D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker 2011. “An Analysis of Underground Forums.” Paper presented at the Internet Measurement Conference (IMC), Berlin, Germany.

Moyer, E. 2019. “‘Darkode’ Goes Dark: Police Shut down Infamous Cybercrime Marketplace.” March 21. https://www.cnet.com/news/darkode-goes-dark-police-shut-down-infamous-cybercrime-marketplace

Norbutas, L. 2013. *AlphaBay cryptomarket scrapes 2013* [Web scrapes].

Onaolapo, J., E. Mariconti, and G. Stringhini. 2016. “What Happens after You are Pwnd: Understanding the Use of Leaked Webmail Credentials in the Wild.” Paper presented at the Proceedings of the 2016 Internet Measurement Conference, Santa Monica, California, USA.

Pino, N. W. 2005. “Serial Offending and the Criminal Events Perspective.” *Homicide Studies* 9 (2): 109–148. doi:10.1177/1088767904271435.

Przepiorka, W., L. Norbutas, and R. Corten. 2017. “Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs.” *European Sociological Review* 33 (6): 752–764. doi:10.1093/esr/jcx072.

Samtani, S., R. Chinn, and H. Chen. 2015. “Exploring Hacker Assets in Underground Forums.” Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on, 1–6. doi:10.1109/ISI.2015.7165935.

Shay, R., I. Ion, R. W. Reeder, and S. Consolvo. 2014. “‘My Religious Aunt Asked Why I Was Trying to Sell Her viagra’: Experiences with Account Hijacking.” Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, Ontario, Canada.

Shulman, A. 2010. “The Underground Credentials Market.” *Computer Fraud & Security* 2010 (3): 5–8. doi:10.1016/S1361-3723(10)70022-1.

Smirnova, O., and T. J. Holt. 2017. “Examining the Geographic Distribution of Victim Nations in Stolen Data Markets.” *American Behavioral Scientist* 61 (11): 1403–1426. doi:10.1177/0002764217734270.

Stone, J. 2015. “What Is Pastebin? How A Quiet Site For Coders Got Thrust Into The Limelight By Hackers.” *International Business Times*, January 29. http://www.ibtimes.com/what-pastebin-how-quiet-site-coders-got-thrust-limelight-hackers-1798264

Van Hardeveld, G. J., C. Webber, and K. O’Hara (2016). “Discovering Credit Card Fraud Methods in Online Tutorials.” Paper presented at the OnSt16, Hannover, Germany.

Villalva, D. A. B., J. Onaolapo, G. Stringhini, and M. Musolesi. 2018. “Under and over the Surface: A Comparison of the Use of Leaked Account Credentials in the Dark and Surface Web.” *Crime Science* 7 (1): 1–17. doi:10.1186/s40163-018-0092-6.

Weaver, G. S., J. E. C. Wittekind, L. Huff-Corzine, J. Corzine, T. A. Petee, and J. P. Jarvis. 2004. “Violent Encounters: A Criminal Event Analysis of Lethal and Nonlethal Outcomes.” *Journal of Contemporary Criminal Justice* 20 (4): 348–368. doi:10.1177/1043986204269381.

Xylitol. 2013. “Darkode Leak.” http://www.xylibox.com/2013/04/darkode-leak.html

Yip, M., C. Webber, and N. Shadbolt. 2013. “Trust among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing.” *Policing and Society* 23 (4): 516–539. doi: 10.1080/10439463.2013.780227.